Claims:

1. An anti-piracy method comprising:

encapsulating a private key in a hardware platform;

requesting content by providing a content request and a public key to a transaction manager;

obtaining the requested content;

encrypting the requested content such that the encrypted content can be decrypted using the private key;

providing the encrypted content to the hardware platform; and

decrypting the encrypted content using the private key to produce a decrypted digital content.

2. The method of claim 1 further including a step of encoding the requested content before encrypting.

3. The method of claim 2 further including converting the decrypted digital content into an analog signal.

4. The method of claim 3 wherein said encrypting step comprises watermarking the requested content.

5. The method of claim 4 wherein watermarking adds traceable information.

6. The method of claim 1 wherein the requested content is retrieved from memory before encrypting.

7. The method of claim 1 wherein the retrieved content is pre-encoded.

8. The method of claim 1 wherein the encrypted content includes play-limiting instructions.

9. An anti-piracy method comprising:

encapsulating a private key in a hardware platform;

requesting broadcast content and providing a content provider with a public key;

encrypting the broadcast content using a broadcast key such that it can be decrypted using the broadcast key;

encrypting the broadcast key using the public key such that the broadcast key can be decrypted using the private key;

sending the encrypted broadcast key and the encrypted broadcast content to the hardware platform;

decrypting the encrypted broadcast key within the hardware platform using the private key; and

decrypting the encrypted broadcast content using the decrypted broadcast key.

10. An anti-piracy system comprising:

an integrated module containing a public key and a private key, said integrated module for receiving encrypted content; and

a manager for receiving a specific content request and public key information, for retrieving the specific content from a storage, and for encrypting the retrieved specific content so that it can be decrypted by said private key;

wherein said integrated module and said manager inter-operatively interact.

11. The system of claim 10 wherein said integrated module and said manager inter-operatively interact using the Internet.

12. The system of claim 10 wherein the integrated module physically encapsulates the private key.

13. An anti-piracy system comprising:

an integrated module containing a public key and a private key, said integrated module for transmitting a broadcast request and the public key and for receiving content; and

a manager for receiving the broadcast request and the public key; wherein the manager includes a broadcast key and a key encrypter for encrypting the broadcast key using the public key such that the broadcast key can be decoded by the private key, wherein the manager further includes a content encrypter for encrypting encoded content using the broadcast key and for transmitting the encrypted content;

wherein the integrated module and the manager inter-operatively interconnect;

wherein the integrated module includes a key decrypter for decrypting the encrypted broadcast key;

wherein the integrated module includes a broadcast decoder for decoding the decrypted broadcast using the broadcast key; and

wherein the integrated module converts the decrypted broadcast content into an analog output.

14. A system of claim 13 wherein the key encrypter changes the encrypted broadcast key within the encrypted content.

15. An integrated module, comprising:

an embedded private key;

a public key mathematically linked to said private key;

a decrypt section for receiving and decrypting an encrypted bitstream using the private key;

a decoder for decoding the decrypted bitstream into decoded digital content;

a digital-to-analog converter for converting the decoded digital content into an analog signal; and

a public key section for sending the public key to an external receiver such that the public key becomes available for encrypting content such that the encrypted content can be decrypted using said private key;

wherein the decrypted bitstream and the decoded digital content are physically encapsulated.

16. An integrated module, comprising:

an embedded private key;

a transmitter for sending a public key that is mathematically linked to said private key;

a key decrypter for receiving and decrypting an encrypted broadcast key using the private key;

a broadcast decrypter for decrypting an encrypted broadcast bitstream into digital content using the decrypted broadcast key;

a decoder for decoding the decrypted broadcast bitstream into decoded digital content; and

a digital-to-analog converter for converting the decoded digital content into an analog signal.

17. The integrated module of claim 16 wherein the decrypted bitstream and the decoded digital content are encapsulated.

18. A system manager comprising:

an input system for receiving a content request and a public key;

a database for storing content;

a processor for retrieving specific content from the database based on the content request; and

an encryption section for encrypting the specific content based on the public key onto an output such that the encrypted content can be decrypted using the private key.

19. A broadcast manager comprising:

an input port for receiving a content request and a public key;

a key encrypter for encrypting a broadcast key based on the public key such that the broadcast key can be decrypted using an associated private key;

a broadcast content provider for providing a broadcast content;

a broadcast encrypter for encrypting the broadcast content such that the broadcast content can be decrypted using the broadcast key; and

an output port for transmitting the encrypted broadcast content and the encrypted broadcast key.

20. A content protection method comprising:

encapsulating a private key and a public key;

transmitting the public key and a content request;

receiving encrypted content in response to the transmitted public key and content request;

decrypting the received encrypted content into a bitstream using the private key;

decoding the decrypted bitstream into decoded digital content; and

converting the decoded digital content into an analog signal.

21. A content protection method comprising:

encapsulating a private key and a public key;

transmitting the public key and a content request;

receiving an encrypted broadcast key;

decrypting the encrypted broadcast key to determine the broadcast key;

receiving encrypted content;

decrypting the encrypted content using the decrypted broadcast key into decrypted digital content; and

converting the decoded digital content into an analog signal.

22. A content protection method comprising:

receiving a content request and a public key;

accessing stored content based on the content request;

encrypting the accessed content based on the received public key such that the encrypted content can be decrypted using an associated private key; and

transmitting the encrypted content.

23. A content protection method comprising:

receiving a content request and a public key;

encrypting a broadcast key based on the public key such that the broadcast key can be decrypted using an associated private key;

accessing broadcast content;

encrypting the broadcast content such that the broadcast content can be decrypted using the decrypted broadcast key; and

transmitting the encrypted broadcast content and the encrypted broadcast key.